Saint Louis University Law Journal

Volume 46
Number 1 *(Winter 2002)*

Article 4

2-12-2002

Balancing Communal Goods and Personal Privacy Under a National Health Informational Privacy Rule

Lawrence O. Gostin
Georgetown University Law Center

James G. Hodge Jr.
Johns Hopkins School of Public Health

Mira S. Burghardt

BALANCING COMMUNAL GOODS AND PERSONAL PRIVACY UNDER A NATIONAL HEALTH INFORMATIONAL PRIVACY RULE

LAWRENCE O. GOSTIN*, JAMES G. HODGE, JR.**
AND MIRA S. BURGHARDT***

> Every single health care professional, every insurance agent, every researcher, every member of an IRB, every public health official, every pharmacist . . . – *every single person who comes in contact with health care records* must understand why its important to keep them safe, how they can keep them safe, [and] what will happen to them if they do not keep them safe.[1]

INTRODUCTION

On April 14, 2001, President George W. Bush approved the Standards for Privacy of Individually Identifiable Health Information (hereinafter referred to as "health data privacy rule"). These regulations, which represent the first systematic national privacy protections of health information,[2] flow from a Congressional mandate in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[3] HIPAA required that health information privacy protections be implemented either through federal legislation or administrative

* J.D., L.L.D. (Hon); Professor of Law, Georgetown University Law Center; Professor, Johns Hopkins Bloomberg School of Public Health; Director, Center for Law and the Public's Health at Georgetown and Johns Hopkins Universities. The authors would like to acknowledge the research assistance of Auburn Daily, J.D. Candidate, Georgetown University Law Center, 2003.
** J.D., L.L.M.; Adjunct Professor of Law, Georgetown University Law Center; Assistant Scientist, Johns Hopkins Bloomberg School of Public Health; Project Director, Center for Law and the Public's Health at Georgetown and Johns Hopkins Universities.
*** J.D. Candidate, 2002, Georgetown University Law Center; Senior Research Assistant, Center for Law and the Public's Health at Georgetown and Johns Hopkins Universities.

1. Donna E. Shalala, *Health Care Information and Privacy*, 8 HEALTH MATRIX 223, 231 (1998) (emphasis added).

2. *See* Press Release, President George W. Bush (Apr. 12, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/04/20010412-1.html (last visited Oct. 19, 2001); Press Release, Secretary Tommy G. Thompson, Statement by HHS Secretary Tommy G. Thompson Regarding the Patient Privacy Rule (Apr. 12, 2001), *available at* http://www.hhs.gov/news/press/2001pres/20010412.html (last visited Jan. 7, 2001) [hereinafter Press Release, Secretary Thompson].

3. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) [hereinafter HIPAA].

regulation by the Department of Health and Human Services (HHS). The regulations protect the privacy of individually-identifiable health records in any form (including electronic, paper and oral) through disclosure and use limitations, fair information practices, and privacy and security policies that apply to "covered entities" (meaning health providers, health insurance plans and health care clearinghouses) and their business associates.

Privacy safeguards are needed because of the personal nature of health data and the rapid shift from paper to electronic records. The harms of unauthorized disclosures of health information are well rehearsed. Health information used by health providers, insurers and data processors can include intimate details about the patient's mental and physical health as well as social behaviors, personal relationships and financial status.[4] Unwarranted disclosures of this information may lead to societal stigmatization and discrimination. Unauthorized disclosures can also lead to a loss of patient trust in medical providers, resulting in a reluctance to seek medical treatment for some conditions or failure to disclose important information to health professionals.[5]

Privacy concerns are compounded by the shift from paper-based to electronic medical record-keeping in the past two decades. Health information is increasingly accessed, used, disclosed and stored in electronic format. This does not necessarily mean health data are less secure, as electronic systems are in many ways safer than manual systems. Nevertheless, electronic data can be accessed in greater quantities and manipulated in ways that are virtually impossible for manual systems. Thus, while significant benefits may flow from the electronic health information infrastructure, the potential to disclose or reveal sensitive health data has raised individual fears of privacy violations. In one recent survey, over 80% of the public respondents felt they had "lost all control" over their personal information.[6]

Patients concerned about a lack of privacy were unlikely to be comforted by federal protections before the promulgation of the HIPAA rule. Prior to the rule, there had never been systematic national health information protection. While most states have privacy safeguards, they are so variable and incoherent that they are widely regarded as inadequate. Congress's grant of authority to HHS to develop privacy standards offered the promise of a considered and comprehensive regulatory solution to address the concerns of consumers and privacy advocates. The standards endeavor to protect patient privacy by limiting disclosures of individually-identifiable medical information (or

4. *See* Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 490 (1995) [hereinafter Gostin, *Health Information Privacy*].

5. *See id*. at 490-91.

6. *Id*. at 454. *See also* Harris Equifax, *Health Information Privacy Survey* (1993), *available at* http://www.epic.org/privacy/medical/polls.html (last visited Oct. 19, 2001).

"protected health information"(PHI)). Disclosure and use of PHI can only occur upon patient consent. The regulations also implement fair information practices, which have long been a feature of existing federal laws.[7] Fair information practices allow patients to (1) inspect and amend their records, (2) receive notice of covered entities' privacy practices and potential uses and disclosures of health information, and (3) request confidential communications and an accounting of actual disclosures.

Through the regulations, HHS attempts to protect individual privacy while recognizing legitimate needs for such data to process health claims and deliver medical care as well as provide for communal goods (including public health and health research). Concerning uses and disclosures of health data, HHS carves out several important exceptions to the consent requirements:

1) Law enforcement. Law enforcement officials may receive information from covered entities without consent pursuant to a court order, subpoena or other legal order.

2) Judicial and administrative proceedings. A covered entity may disclose PHI in a judicial or administrative proceeding without the individual's consent in response to an order of the court or administrative tribunal or in certain circumstances, a subpoena or discovery request.

3) Commercial marketing. Covered entities may use or disclose personal health information for face-to-face commercial marketing to individuals or regarding products or services of nominal value.

4) Parents of unemancipated minors. Parents are recognized as personal representatives of unemancipated minors. While the rule places certain restrictions on parent's access to the child's medical record, HHS acknowledges that the Bush Administration is likely to relax those limitations.[8]

5) Family members, friends, and caretakers ("significant others") of adults and emancipated minors. Covered entities may disclose limited health information of an adult or emancipated minor without consent to a relative, personal friend or designated person in the case of an emergency or in the course of basic care-taking duties.

6) Public health. PHI can be disclosed for numerous public health purposes without consent, including to (a) prevent or control disease, injury or disability, (b) report child abuse or neglect, (c) report relevant information to the Food and Drug Administration, and (d) report to an employer conducting medical surveillance in the workplace if the employee is notified.

7) Health research. A covered entity can use or disclose PHI for research without consent if it obtains a waiver from an Institutional Review Board (IRB) or a privacy board according to a series of considerations.[9]

7. *See infra* Part II.D. for a discussion of fair information practices.
8. *See* Press Release, Secretary Thompson, *supra* note 2.
9. *See generally* 45 C.F.R. § 164.512 (2001).

Many of these provisions leave significant gaps in privacy protection. HHS admits that the rule only sets a "floor" of protection that "balance[s] the needs of the individual with the needs of society."[10] However, the rule contains many flaws as a base-line standard, promoting inappropriate trade-offs between the public welfare and individual privacy. The rule inadequately protects privacy in certain contexts, including the consent requirements for use and disclosure of PHI for health care purposes and some fair information practices provisions. In contrast, the rule sometimes fails to assure that information can be used when necessary for significant communal benefits or requires substantial burdens on the health care industry without providing meaningful protection for patients.

In Part I, we examine how the threat to personal privacy from the developing electronic health information infrastructure necessitates comprehensive national health information privacy regulations. Attempts by federal and state officials to regulate the use and disclosure of personal health information prior to the new standard have been inadequate because existing legal provisions allow multiple exceptions to privacy prohibitions.

We examine and analyze the framework of HHS's effort to protect individually identifiable electronic health information in Part II. Patients obtain several new rights and protections related to their individually identifiable health information. However, throughout the standard, inappropriate trade-offs between individual privacy and communal goods compromise the strides made for protecting personal health information privacy. A brief conclusion follows.

I. THE ELECTRONIC HEALTH INFORMATION INFRASTRUCTURE AND PERSONAL PRIVACY

A. Health Data in the Electronic Health Information Infrastructure

Protecting the privacy of identifiable health information was one of the key priorities of Congress in enacting the Health Insurance Portability and Accountability Act of 1996. One of the main reasons that Congress desired privacy protection was its concern about the proliferation of electronic health information. During the mid-1980's, fundamental shifts in the organization, delivery and financing of health care services led to the development of more

10. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000). For electronic copies of the health data privacy rule, including the background materials and comments published in the federal register, see the Department of Health and Human Services' website, *available at* http://aspe.hhs.gov/admnsimp (last visited Jan. 7, 2002) or http://www.hhs.gov/ocr/hipaa (last visited Jan. 7, 2002).

sophisticated health information systems.[11] Today, individual patient medical records are increasingly stored in electronic databases by government and private medical providers. The goal that fueled these changes, as expressed by the Institute of Medicine and others, was that patient medical records should be recorded in every health care setting and accessed widely among health care professionals.[12] These changes are transforming how health information is acquired, used, disclosed and stored in the modern health care system.

Many advantages exist to the systemic collection and use of electronic health data. More accurate and accessible data allow consumers to make more informed decisions about health plans, providers, diagnoses, products and treatments. Clinical care is improved through faster and more accurate diagnoses,[13] increased checks on medical procedures,[14] prevention of adverse drug events[15] and the dissemination of expert medical information in areas traditionally under-served through telemedicine and other techniques. Medical research on the causes of disease and injuries and health services research concerning the quality and cost-effectiveness of health care services are improved through increased access to information and more accurate information. Public health surveillance of injuries and diseases in the population is facilitated.[16] Finally, electronic security tools including personal access codes, encryption programs[17] and audit trails[18] can more efficiently monitor health care fraud and abuse[19] and protect data from unauthorized uses and disclosures.

Along with these benefits, however, come significant costs. The computerization of health data raises significant privacy concerns. Health care

11. *See* NATIONAL RESEARCH COUNCIL, COMMITTEE ON MAINTAINING PRIVACY AND SECURITY IN HEALTH CARE APPLICATIONS OF THE NATIONAL INFORMATION INFRASTRUCTURE, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION 21-22 (1997); Lawrence O. Gostin, *Personal Privacy in the Health Care System: Employer-Sponsored Insurance, Managed Care, and Integrated Delivery Systems*, 7 KENNEDY INST. ETHICS J. 361, 364 (1997).

12. *See* Gostin, *Health Information Privacy*, *supra* note 4, at 452-53.

13. *See* Dereck L. Hunt et al., *Effects of Computer-Based Clinical Decision Support Systems on Physician Performance and Patient Outcomes*, 280 JAMA 1339, 1342 (1998).

14. *See* David W. Bates et al., *Effect of Computerized Physician Order Entry and a Team Intervention on Prevention of Serious Medication Errors*, 280 JAMA 1311, 1315 (1998).

15. *See* Robert A. Raschke et al., *A Computer Alert System to Prevent Injury from Adverse Drug Events*, 280 JAMA 1317, 1320 (1998).

16. *See* Lawrence O. Gostin et al., *The Public Health Information Infrastructure*, 275 JAMA 1921, 1921 (1996) [hereinafter Gostin et al., *Genetic Privacy and the Law*]. *See also* Antoine Flahault et al., *FluNet as a Tool for Global Monitoring of Influenza on the Web*, 280 JAMA 1330 (1998).

17. *See* Elizabeth Corcoran, *Breakthrough Possible in Battle over Encryption Technology*, WASH. POST, July 12, 1998, at A8.

18. *See* NATIONAL RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE 88 (1991).

19. *See* Gostin, *Health Information Privacy*, *supra* note 4, at 481.

data about individuals are among the most sensitive types of personal information. These records contain large amounts of personal information which can be used to create a profile of an individual, including 1) demographic information, such as age, sex, race, marital status, children and occupation; 2) financial information, such as employment status, income and methods of payment; 3) medical information about diagnoses, treatments, disabilities, end-of-life decisions and disease histories of the individual and family members; 4) genomic information, such as diagnostic tests for carrier traits and genetically-related diseases; 5) personal identifiers other than name, including Social Security number, addresses and phone numbers; and 6) information about why treatment is sought, such as being the victim of a violent crime, firearm injury or the at-fault party in an auto accident.[20]

In a society which strongly values individual autonomy and decision-making, protecting the privacy of personally-identifiable health data is critical. Insufficient protections of health care information lead to unauthorized disclosures which may subject individuals to social stigma and discrimination by insurance companies, health care professionals and institutions, and employers.[21] Patients have a reasonable expectation of privacy in their personal affairs provided the exercise of these interests does not harm others.[22] Respecting personal privacy requires that individuals maintain some degree of control over their personal information. In addition, protecting the privacy of individually-identifiable health information is often important to achieve benefits to the population, such as public health surveillance and longitudinal health research. As we (and others) have stated, *protecting health information privacy* (for instance, by providing individuals some control over their health data without severely restricting warranted uses of the data) *directly improves the quality of health care and public health data* (for instance, by encouraging individuals to fully utilize health services and cooperate with health agencies).[23]

20. *See* Lawrence Gostin, *Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations,* 127 ANNALS INTERNAL MED. 683, 684-85 (1997).

21. *See, e.g.*, Lawrence O. Gostin & James G. Hodge, Jr., *The "Names Debate": The Case for National HIV Reporting in the United States*, 61 ALB. L. REV. 679, 724 (1998).

22. TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 126 (4th ed. 1994).

23. James G. Hodge, Jr. et al., *Legal Issues Concerning Electronic Health Information*, 282 JAMA 1466, 1470 (1999).

B. The Inadequacy of Existing Legal Protections

Personal privacy can be safeguarded in several ways, including through the privacy policies of data holders in the public and private sectors.[24] The law, however, is uniquely important because it sets clear standards that are enforceable through courts and administrative bodies. Legal safeguards may be expressed through federal or state constitutional protections of health information privacy, legislation or case law. Despite the law's potential to protect privacy, existing legal safeguards are inadequate, fragmented and inconsistent. There exist major gaps in legal protection of privacy and significant theoretical problems with the structure of privacy protection.

1. Constitutional Right to Privacy

The Supreme Court has not articulated a clear, strong standard for a constitutional right to informational privacy outside the Fourth Amendment.[25] Judicial recognition of a constitutional right to informational privacy is particularly important because the government is a primary collector and disseminator of health information. A constitutional right would help shield individuals from unauthorized government acquisition or disclosure of personal information.

The Constitution does not expressly provide a right to informational privacy.[26] The judiciary, however, has recognized a limited right to informational privacy as a liberty interest within the Fifth and Fourteenth Amendments. In *Whalen v. Roe*,[27] the United States Supreme Court examined

24. The law is merely one tool to improve individual privacy protections. Internal privacy policies of health care providers, data processors and other private sector entities, which acquire, use and disclose identifiable health data can greatly impact individual expectations of the privacy of their health information. The same can be said for voluntarily-executed policies of governmental holders of data, including public health agencies, researchers, universities and academic centers, and other commissions or agencies. Adherence to ethical principles and human rights documents in support of the privacy of individual health data may also lead to greater privacy protections. Ultimately, however, where government and the private sector fail to administer sufficient privacy protections, the law may guide, if not require, such protections.

25. *See generally*, Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1 (1991); Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479 (1990); Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133 (1991).

26. *See* Gostin, *Health Information Privacy*, *supra* note 4, at 495.

27. 429 U.S. 589 (1977); *see also* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 465 (1977). In *Nixon*, the court held that while the President has

> a legitimate expectation of privacy in his personal communications . . . the constitutionality of the Act must be viewed in the context of the limited intrusion of the screening process, of appellant's status as a public figure, of his lack of any expectation of privacy in the overwhelming majority of the materials, of the important public interest in

whether the constitutional right to privacy encompasses the collection, storage and dissemination of health information in government data banks (specifically, a New York public health database containing pharmaceutical records). While the Court acknowledged a "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files,"[28] it failed to tailor a constitutional remedy to meet this threat. Justice Stevens, writing for a unanimous Court, simply recognized that "in some circumstances" the duty to avoid unwarranted disclosures "arguably has its roots in the Constitution."[29] Provided the state has adequate standards and procedures for protecting the privacy of sensitive medical information, the Court found no privacy violation.[30] *Whalen* has been subsequently interpreted as affording a tightly circumscribed right to informational privacy.

In general, courts have employed a flexible test balancing the government invasion of privacy against the strength of the government interest.[31] Where the government can articulate a valid societal purpose and employs reasonable security measures, traditional governmental activities of information collection are deemed not to infringe upon constitutional informational privacy rights. Any right to privacy under the federal or state constitutions[32] is, of course, limited to state action. Thus, collection and use of health data by private or quasi-private health data organizations, health plans researchers and insurers is constitutionally unprotected.

> the preservation of the material, and of the virtual impossibility of segregating the small quantity of private materials without comprehensive screening . . . the appellant's privacy claim is without merit.

Id.

28. *Whalen*, 429 U.S. at 605.

29. *Id.*

30. *Id.*

31. For example, the court in *United States v. Westinghouse Electric Corp.* held that the National Institute of Occupational Safety and Health was entitled to receive the medical records of private employees exposed to toxic substance, subject to their informed consent. 638 F.2d 570, 578 (3d Cir. 1980). The court enunciated five factors to be balanced in determining the scope of the constitutional right to informational privacy: (1) the type of record and the information it contains, (2) the potential for harm in any unauthorized disclosure, (3) "the injury from disclosure to the relationship in which the record was generated," (4) "the adequacy of safeguards to prevent unauthorized disclosure," and (5) "the degree of need for access"—meaning, a recognizable public interest. *Id*.

32. *See, e.g.*, Rasmussen v. S. Fla. Blood Serv., Inc., 500 So. 2d 533 (Fla. 1987). Since the 1970s, more than a dozen states have adopted constitutional amendments designed to protect a variety of privacy interests, including limitations on access to personal information. *See* Gostin, *Health Information Privacy*, *supra* note 4, at 498.

2. Common Law Protections

Most states recognize via common and statutory law the legal duties of confidentiality of certain health care professionals (including physicians, nurses and lab technicians) not to disclose health information. Yet, these duties are not absolute: "Disclosures without individual consent may lawfully be made to [1] protect third parties from identifiable harm, [2] to report information for public health purposes as required by state law, or [3] sometimes in cases of medical emergency. Unwarranted disclosures, however, may subject responsible parties to civil liability . . . ."[33]

Although a traditional construct of privacy protections and a forerunner of modern privacy theory, the duty of confidentiality is antiquated. Confidentiality is predicated on the existence of a physician/patient relationship. However, modern data collection is based only in small part on this relationship. Health records contain a substantial amount of information gathered from numerous primary and secondary sources: laboratories, pharmacies, schools, public health officials, researchers, insurers and other individuals and institutions. Paper or electronic patient health records are not merely kept in the office of private physicians or health plans, but also by government agencies, regional health database organizations and information brokers. The duty of confidentiality arising at the point of clinical care or research simply does not convey a right to confidentiality in all these important contexts.

3. Existing Legislative and Administrative Protections

Federal and state legislatures and executive agencies have enacted and considered a growing number of statutes and regulations to protect privacy.[34] The federal government has previously enacted several statutes and regulations to protect privacy of health information. The Privacy Act of 1974[35] requires federal agencies to utilize fair information practices regarding the collection, use or dissemination of systematized records, including health data. The Freedom of Information Act (FOIA) of 1966[36] requires the federal government to disseminate various information but exempts several categories of records, including personally-identifiable health information. Other federal regulations protect health information privacy relating to the treatment of persons for drug

33. Lawrence O. Gostin & James G. Hodge, Jr., *Genetic Privacy and the Law: An End to Genetics Exceptionalism*, 40 JURIMETRICS 21, 46 (1999) [hereinafter Gostin & Hodge, *Genetic Privacy and the Law*]. *See also* McCormick v. England, 494 S.E.2d 431, 439 (S.C. Ct. App. 1997); Gostin, *Health Information Privacy*, *supra* note 4, at 508-11.

34. For a discussion of various regulations enacted to protect privacy, see Gostin, *Health Information Privacy*, *supra* note 4, at 499-508.

35. 5 U.S.C. § 552a (2000).

36. 5 U.S.C. § 552 (b)(1)-(3) & (6) (1988).

or alcohol dependency in federally-funded facilities[37] and the administration of human subject research.[38]

Most states have passed privacy statutes that mimic the Federal Privacy Act[39] and FOIA,[40] and thus apply only to state collections of data. A few states have enacted comprehensive medical information privacy acts.[41] These laws provide broad protections of health information acquired, collected, used or disclosed within the state. States have also passed disease-specific privacy laws which set forth stringent privacy and security protections for certain types of information, including medical information concerning one's HIV status[42] or other sexually-transmitted diseases,[43] genetic information,[44] information utilized in medical research (such as state cancer registries) or public health information.[45]

Though existing federal and state privacy statutes and regulations are meaningful and serve valuable ends, they share several weaknesses: (1) like constitutional privacy protections, most statutes apply primarily to government collections, uses or disclosures of health information, and thus often do not confer protections to health information in the private sector; (2) they fail to address the new challenges to individual privacy arising from the automation of medical records; (3) they collectively represent a patchwork effort to address the privacy and security of specific health information or information held by specific entities, and thus do not comprehensively protect health information; (4) some kinds of data are treated as super-confidential (for instance, HIV/AIDS), while other data are virtually unprotected, leading to inconsistencies and unfairness; (5) they do not effectively balance competing individual interests in privacy with the need to use the data for the common good; and (6) some state laws prohibit disclosures without informed consent, but list so many exceptions as to swallow the rule. These weaknesses in existing law require a national approach to privacy protection. The health data privacy rule provides such a national standard and makes significant strides in protecting health data. However, the rule shares many of the weaknesses of existing privacy laws. In some ways, the rule inadequately protects privacy,

37. 42 U.S.C. § 290dd-2 (Supp. V 1994).

38. 45 C.F.R. § 46.111(7) (1993).

39. *See, e.g.*, N.Y. PUB. OFF. LAW §§ 91-99 (McKinney 2001).

40. *See, e.g.*, MISS. CODE ANN. §§ 25-61-1 (1972).

41. *See, e.g.*, CAL. CIV. CODE §§ 56-56.35 (West 1982 & Supp. 2001); WASH. REV. CODE ANN. §§ 70.02.005-70.02.904 (West 1992 & Supp. 2001).

42. *See generally* Harold Edgar & Hazel Sandomire, *Medical Privacy Issues in the Age of AIDS: Legislative Options*, 16 AM. J.L. & MED. 155 (1990) (examining state legislation dealing with HIV related problems in medical privacy laws).

43. *See* Lawrence O. Gostin, *The Future of Public Health Law*, 12 AM. J.L. & MED. 461, 486 (1986).

44. *See, e.g.*, Gostin & Hodge, *Genetic Privacy and the Law*, *supra* note 33, at 47.

45. *See* Gostin et al., *Genetic Privacy and the Law*, *supra* note 16, at 1922.

while in other ways it fails to assure that data are shared where necessary to protect the public's welfare.

II. PROTECTING PERSONAL PRIVACY IN THE NEW STANDARD

The creation of a national health information privacy rule might seem uncontroversial in light of existing public apprehensions, current gaps in legal protections and Congress's commitment to better protecting such data. However, the health privacy rule was established only after years of struggle and efforts in the legislative and executive branches. In HIPAA, Congress created a self-imposed deadline of August 21, 1999 to pass health information privacy legislation.[46] Due in part to the lobbying of the various interest groups affected by such legislation,[47] Congress failed to reach a consensus by the deadline.[48] In default, HIPAA authorized the Secretary of the HHS to issue privacy regulations if Congress failed to meet the deadline.[49] After issuing a proposed rule in November, 1999,[50] HHS received over 50,000 public comments.[51] The final rule was promulgated in December, 2000 at the end of President Clinton's term.[52] Reflecting President Bush's promise to reassess regulations enacted late in his predecessor's term,[53] the comment period was re-opened and HHS received several thousand additional comments.[54] Though privacy advocates were concerned that the Bush Administration would scale back or eliminate the rules altogether,[55] HHS Secretary Tommy Thompson

46. HIPAA, Pub. L. No. 104-191, § 264(c)(1) (1996).

47. *See* Amy Goldstein & Robert O'Harrow, *Bush will Proceed on Patient Privacy; But Clinton-Era Rules Likely to be Modified*, WASH. POST, Apr. 13, 2001, at A1. This, however, is nothing new. A 1998 Center for Public Integrity report found that "[t]ime and time again . . . Congress has put big-money corporate interests ahead of the basic privacy interests of the American people." THE CENTER FOR PUBLIC INTEGRITY, NOTHING SACRED: THE POLITICS OF PRIVACY (1998), *available at* http://publicintegrity.org/nothing_sacred.html (last visited Nov. 4, 2001).

48. *See* Press Release, U.S. Department of Health and Human Services, Protecting the Privacy of Patients' Health Information (May 9, 2001), *available at* http://aspe.hhs.gov/admnsimp/final/pvcfact2.htm [hereinafter HHS Press Release]; Goldstein & O'Harrow, *supra* note 47.

49. HIPAA, Pub. L. No. 104-191, § 264(c)(1) (1996).

50. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (Nov. 13, 1999).

51. *See* HHS Press Release, *supra* note 48.

52. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000).

53. *See* Robert Pear, *Bush Accepts Rules to Protect Privacy of Medical Records*, N.Y. TIMES, Apr. 13, 2001, at A1 [hereinafter Pear, *Bush Accepts Rules*].

54. *See* Press Release, Secretary Thompson, *supra* note 2; HHS Press Release, *supra* note 48.

55. *See* HEALTH PRIVACY PROJECT, COMMENTS ON THE FINAL FEDERAL STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION 3 (2001), *available at*

announced on April 12, 2001, that the final rule as previously constructed would go forward, subject to interpretive guidelines developed by HHS.[56] The first of these guidelines was released in July, 2001, with Secretary Thompson intending to write more.[57] The rules take effect for most covered entities on April 12, 2003, and a year later for small health plans.

Despite its convoluted development, the health data privacy rule provides a variety of privacy protections for health care consumers.[58] The standard applies to covered entities, such as health care plans, health care clearinghouses and health providers, along with their business entities.[59] HHS regulates individually-identifiable health information, meaning PHI, derived from electronic, written and oral communications.[60] Uses and disclosures are subject to consent requirements, so as to prevent harmful sharing of PHI. These consent requirements are of two broad types: (1) informed consent provisions relating to the use of health data for transactions that are standard in the delivery and payment of health care services; and (2) authorization requirements for disclosures of PHI for non-health care purposes.[61]

Trade-offs between public good and personal privacy are manifested in certain exceptions to the authorization requirements for outside disclosures. In general, PHI may not be disclosed without specific, written authorization, except: (1) to law enforcement officials; (2) to judicial and administrative proceedings; (3) for commercial marketing purposes; (4) to parents of unemancipated minors; (5) to "significant others," such as family members,

http://www.healthprivacy.org/usr_doc/55009.pdf (last visited Jan. 7, 2001) [hereinafter HEALTH PRIVACY PROJECT, COMMENTS]; *see also* Goldstein & O'Harrow, *supra* note 47; Robert Pear, *White House Plans to Revise New Medical Privacy Rules*, N.Y. TIMES, Apr. 8, 2001, at 22.

56. Press Release, Secretary Thompson, *supra* note 2; *see* Goldstein & O'Harrow, *supra* note 47; Pear, *Bush Accepts Rules*, *supra* note 53.

57. Office for Civil Rights, Department of Heath and Human Services, Standards for Privacy of Individually Identifiable Health Information, *available at* http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm (last modified July 6, 2001) [hereinafter Office for Civil Rights Standards]. *See* Ceci Connelly, *Guidelines on Patient Privacy Rules Issued; Administration Postpones Action on Parents' Access to Minors' Health Records*, WASH. POST, July 7, 2001, at A6; Robert Pear, *Administration Clarifies New U.S. Rules Guarding Privacy of Patients*, N. Y. TIMES, July 7, 2001, at A9.

58. To enforce these protections, the Secretary of HHS can investigate complaints and conduct compliance reviews. *See* 45 C.F.R. §§ 160.306, 160.308 (2001). Violations of the standard can lead to civil and criminal penalties up to $250,000 and ten years in prison. *See* HHS Press Release, *supra* note 48. There is no private right of action for individuals to redress violations.

59. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,475 (Dec. 28, 2000).

60. Unless the context otherwise requires, all further references to health information refer only to individually-identifiable data.

61. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,509.

close friends, or designated persons, of an adult or emancipated minor, (6) to an authorized public health authority, and (7) for health research.[62]

The rule also requires covered entities to develop privacy and security policies to protect stored health information. Fair information practices set forth in the rule include a patient's right to: (1) receive notice of covered entities' privacy practices and potential uses and disclosures of health information;[63] (2) review one's PHI;[64] (3) request amendments to one's PHI;[65] and (4) request confidential communications and an accounting of actual disclosures.[66] The regulation generally does not preempt any state law that is more stringent than the health data privacy rule.[67] Thus, states may impose stricter privacy provisions.

As will be discussed below, the rule endeavors to set a national base-line of health information privacy protection. Individual privacy, however, is sometimes under-protected or overprotected within that standard.

A. The Scope of the Standard

At least two questions arise in the development of a national health information privacy standard. First, what information should be protected? Secondly, from whose actions should the information be protected? In the health data privacy rule, these questions are partially answered by the limits of HHS's authority under HIPAA.[68]

1. Protected Health Information (PHI)

The regulation explicitly covers health information[69] that is individually-identifiable.[70] Individually-identifiable health information includes any data

62. *See generally* 45 C.F.R. § 164.512 (2001). In the interest of space and concise discussion, this Article focuses on the most controversial and significant exemptions to the consent requirements. However, the rule contains additional exemptions for treatment emergencies, communication difficulties between patient and provider, legal mandates for treatment, health oversight activities, decedents, serious threats to health or safety and military and veteran's activities. *See id.* §§ 164.506(a)(3)(i), 164.512.

63. *See* § 164.520(a).

64. § 164.524(a).

65. § 164.526(a).

66. § 164.528(a).

67. § 160.203(b).

68. For a discussion on the constitutional issues raised because of jurisdictional concerns related to HIPAA, see A. Craig Eddy, *A Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of The Health Insurance Privacy and Accountability Act of 1996*, 9 ANNALS HEALTH L. 1, 50-60 (2000).

69. "Health information" is comprehensively defined as data

> (1) . . . created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) [r]elate[d] to the past, present, or future physical or mental health or condition of an

that contains unique identifiable characteristics, including a name, social security or driver's license number, fingerprint and genetic link.[71] Where health data are truly non-identifiable, there are no individual privacy implications relating to its access, use or disclosure. Thus, such data require no privacy protection. Excluding non-identifiable health data (for example, aggregate statistical data, non-linked data or other data stripped of all individual identifiers) provides an incentive for data holders to use or de-identify health information to diminish the risk of harmful disclosures and uses of personal data.[72] Under the standard, HHS permits covered entities to assign codes[73] to allow for later re-identification but requires steps be taken to prevent harmful identifications.[74]

HHS defines PHI to include all forms of information, including electronic, oral and paper communications.[75] It is impractical to separate protections for

individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

§ 160.103.

70. § 164.514 (discussing procedures for de-identification of health information). HHS defines individually-identifiable health information as health information which "identifies an individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual." § 164.501. The regulatory definition limits the term to only a subset of health information, specifically that created or received by health care providers, health plans, employers or health care clearinghouses. *See id.*

71. The health data privacy rule outlines two means for determining if health information is not individually-identifiable ("de-identified") and thus no longer regulated by the rule. First, an expert utilizing accepted analytic techniques can conclude that "the risk is very small that the information could be used, alone or in combination with other reasonably available information" to identify the subject of the information. § 164.514(b)(1). A second permitted means of de-identification is that the covered entity can remove a comprehensive set of identifiers of the individual and of relatives, employers and household members of the individual. These identifiers include names, geographic subdivisions smaller than a state, dates more specific than years, contact information such as telephone and fax numbers and email addresses, identification numbers such as social security numbers, account and medical record numbers, license place numbers and full face photographic images. § 164.514(b)(2)(i).

72. *See* HEALTH PRIVACY PROJECT, BEST PRINCIPLES FOR HEALTH PRIVACY 15-16 (1999), *available at* http://www.healthprivacy.org/usr_doc/33807.pdf (last visited Nov. 4, 2001) [hereinafter HEALTH PRIVACY PROJECT, BEST PRINCIPLES]; HEALTH PRIVACY PROJECT, COMMENTS, *supra* note 55, at 18.

73. Information can be "ostensibly anonymous," yet linkable to an individual because of codes frequently utilized by health care organizations, researchers and the government. Concern is raised about deliberate or accidental disclosures of coded information, not literally protected by law, where the code is broken or inadequate. Gostin, *Health Information Privacy*, *supra* note 4, at 520.

74. The code must not be derived from or related to information about the individual or able to be translated so that the individual can be identified. *See* § 164.514(c)(1). The covered entity must also not disclose or use the code for other purposes than record identification and cannot disclose the mechanism for re-identification. *See* § 164.514(c)(2).

75. § 164.501 (defining "protected health information").

paper-based records from electronic or oral-based data. HHS's attempt to cover all types of health data, however, is controversial. Congress may not have granted clear authority to HHS to regulate non-electronic communication in HIPAA.[76] Although HHS maintains it has "ample legal authority" to regulate non-electronic communications,[77] the regulation is structured so that non-electronic communications are severable by court action from electronic communications.[78] Alternatively, by protecting all health information, the efficacy of the regulation would be enhanced. Otherwise, a significant amount of non-electronic health communications would remain unregulated by federal law. There would be complications in enforcing a national standard applicable to only some types of health data, depending on how they were communicated or stored.[79]

2. Covered entities.

HHS regulates the actions of "covered entities" that it has authority to reach under HIPAA. These "covered entities" include health plans, health care

76. Section 264 of HIPAA, which contains the Congressional mandate to HHS to develop the privacy standard, evolved because of the administrative simplification goals of the statute related to electronic information exchange. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,469 (Dec. 28, 2000); *see also* Eddy, *supra* note 68, at 18. Some commentators have suggested that because section 264 was developed to counteract negative effects of the administrative simplification provisions, HHS could only regulate privacy concerns for the narrow set of electronic transactions covered in those provisions. *See* Eddy, *supra* note 68, at 19-20. However, section 264 of HIPAA describes the scope of HHS authority in terms of regulation of individual rights over "individually identifiable health information," not electronic transactions or administrative simplification. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 2033 (1996). The statute states that if Congress does not meet its deadline, HHS must "at least" develop regulations that address: "(1) [t]he rights that an individual who is a subject of individually identifiable health information should have[;] (2) [t]he procedures that should be established for the exercise of such rights[; and] (3) [t]he uses and disclosures of such information that should be authorized or required." *Id.* This subsection provides the requirements for HHS's recommendation to Congress when Congress is considering legislation before its self-imposed deadline has passed. Based on a cross-reference to 264(b), 264(c) applies these requirements to the regulations that are mandated if Congress does not meet its deadline. *See id*. The use of "at least" and the lack of a reference to the administrative simplification sections or electronic transactions in these detailed requirements suggests that Congress did not intend to limit HHS to protecting privacy in electronic transactions only. *See* HEALTH PRIVACY PROJECT, COMMENTS, *supra* note 55, at 5. Nevertheless, ambiguity remains about HHS's scope of authority.

77. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,496.

78. *See id.* In a successful court challenge to the broad coverage, then the judge could order that the phrase "regarding non-electronic information" be struck from the regulation while the standard would remain intact for electronic communications.

79. *See* HEALTH PRIVACY PROJECT, COMMENTS, *supra* note 55, at 6-7.

clearinghouses and health care providers.[80] Health plans, which provide or pay for the cost of medical care, are covered whether they are private entities (such as a health insurer or managed care organization) or government organizations (such as Medicaid, Medicare or the Veterans Administration).[81] Health care providers (meaning physicians, hospitals or clinics) are covered if they "[transmit] any health information in electronic form in connection with a transaction covered by [the regulation]."[82] Such electronic exchanges can include billing and fund transfers in addition to health information communications.

The rule also covers business associates of the covered entities. Business associates are lawyers, accountants, billing companies and other contractors whose positions involve the use or disclosure of individually-identifiable health information.[83] Although HHS lacks the authority to directly regulate business associates, it requires covered entities to obtain "satisfactory assurance[s] that [their] business associates will appropriately safeguard the information."[84] Should a covered entity know of a violation and do nothing to address it, the covered entity may be considered to have violated HIPAA's privacy standards.[85] While covered entities have protested that this is unfair, this technique was maintained by HHS in the final rule as a way to regulate the downstream users and processors of PHI.[86]

Though the regulations are facially comprehensive in their coverage, not all persons or entities who regularly use, disclose or store identifiable health data are covered. For example, the rule does not cover groups such as life insurance companies or worker's compensation insurance companies and programs, even though these entities regularly use personal medical information.[87] Additional protections governing all identifiable health data,

80. § 160.102(a).

81. § 160.103 (defining "health plan"). Employers utilizing employer-sponsored health plans, governed by ERISA, are not considered covered entities when administering the plan (as "plan sponsors"). *Id.* (listing exclusions to the definition of "health plan"). However, the standard outlines numerous requirements for employer-sponsored health plans, as covered entities, to disclose PHI to plan sponsors/employers, including an agreement that the sponsor will not use or disclose the information for employment decisions. § 164.504(f)(1)-(2) (2001).

82. § 160.102(a)(3).

83. *See* § 160.103.

84. § 164.502(e)(1)(i).

85. *See* § 164.502(e)(1)(iii).

86. *See* Lawrence O. Gostin, *National Health Information Privacy: Regulations Under the Health Insurance Portability and Accountability Act*, 285 JAMA 3015, 3016 (2001) [hereinafter Gostin, *Regulations under HIPAA*].

87. *See generally* James G. Hodge, Jr., *The Intersection of Federal Health Information Privacy and State Administrative Law: The Protection of Individual Health Data and Worker's Compensation*, 51 ADMIN. L. REV. 117 (1999).

regardless of the holder or manner of communication, are needed to complete a national standard of health information privacy.

B. Consenting to Uses and Disclosures of Protected Health Information

Regulating the use and disclosure of PHI is essential in assuring patients' privacy because of the potential risk of harm from unlimited sharing of personal medical data. Requiring informed consent for uses and disclosures allows individuals some degree of control over their individually-identifiable health information. HHS augments consent protections by imposing a minimum disclosure standard that limits the amount of information that can be shared. The standard requires that when using, disclosing or requesting PHI, the covered entity must make reasonable efforts to limit the disclosure to the minimum amount of information necessary to accomplish an otherwise lawful purpose.[88] Collectively, these measures can enhance patient autonomy and promote trust in the health care system.[89] The minimum disclosure standard helps patients maintain their privacy in transactions, such as reimbursement, where only specific health information is required and additional disclosures could lead to harm to patients.[90] Informed consent mechanisms are featured in the health data privacy rule with mixed success. Written authorization requiring disclosures of health data for non-health care purposes is effective in protecting individual privacy. However, written consent requiring disclosures for treatment, payment and health care operations fails to protect individuals and burdens covered entities.

1. Written Consent for Disclosure and Use for Health Care Purposes

The consent rule requires covered health care providers to obtain written consent from individuals before using or disclosing information for treatment, payment or health care operations. Such consent must (1) be in plain language,[91] (2) inform the individual that PHI may be used and disclosed to

88. § 164.502(b)(1).

89. *See* Gostin, *Health Information Privacy*, *supra* note 4, at 522. For further discussion, see HEALTH PRIVACY PROJECT, COMMENTS, *supra* note 55, at 22-33 (arguing that personally identifiable health information should not be disclosed without authorization except in limited circumstances).

90. HHS's recent guidance has clarified a significant concern of health care providers over the permitted uses during treatment when consulting with other physicians or medical staff. The standard as written specifies that the minimum disclosure requirement applies for use of PHI during treatment by health care providers, but not disclosures. This has caused confusion about how health care providers can utilize vital health information in the course of treatment as they work with other medical professionals. In the July, 2001 guidance, HHS explained that the exemption for disclosures during treatment allows health care providers to share information with other providers. *See* Office for Civil Rights Standards, *supra* note 57.

91. § 164.506(c).

carry out those activities,[92] (3) indicate that the individual can revoke the consent in writing[93] and (4) state that the individual may request that the covered entity restrict how PHI is used or disclosed for health care purposes, though the covered entity is not required to agree.[94] Certain exceptions for specific disclosures are discussed below.

The written consent requirement for use and disclosure of PHI in health care activities is largely inadequate.[95] Consent under these circumstances is neither informed nor consensual. A patient may sign a consent form on his first visit to a physician that applies to all future disclosures and uses. In such cases, the individual will not be aware of the substance of the data protected because he will typically not know what information is contained in his current records, or what may be contained in his future medical records.[96] At the time of consent, he will also not be aware of the specific uses or disclosures because the consent form need only state "treatment, payment, or health care operations."[97] For these reasons, his execution of a written authorization prior to treatment is uninformed. Such authorization also lacks effective consent where the rule allows providers to condition enrollment in a plan or medical treatment on whether the individual signs the consent.[98] As a result, the patient can be forced to consent if he wants to obtain treatment or health insurance.[99]

The written consent requirement also creates significant burdens for the health care industry. While many health providers already maintain individual informed consent as part of most health care transactions, all covered entities will have to develop mechanisms to obtain, access and store consent forms from every individual. Health care providers have the additional concern of having to delay treatment because consent forms are lost or unsigned.[100]

92. § 164.506(c)(1)-(2). The consent may not be combined in a single document with the notice. § 164.506(b)(3).

93. § 164.506(c)(5).

94. § 164.506(c)(4). If the covered entity does agree, the agreement is binding. *See* § 164.522(a) (restating the standard for an individual's right to request restrictions of uses and disclosures and documenting the requirements for termination of the restrictions).

95. Note that the consent requirement was not in the proposed rule.

96. *See* Gostin, *Regulations under HIPAA*, *supra* note 86, at 3017.

97. § 164.506(c)(1).

98. § 164.506(b)(1)-(2).

99. *See* HEALTH PRIVACY PROJECT, COMMENTS, *supra* note 55, at 22.

100. *See id.* A further burden is placed on the practices of pharmacists. As the regulation is currently written, pharmacists cannot use PHI to fill a prescription that was telephoned by the individual's doctor if the patient is a new patient to the pharmacy and has not given written consent to the pharmacy. HHS has indicated in the guidance issued in July, 2001 that this is an undesirable outcome and it plans to issue a proposed rule to rectify this concern. Office for Civil Rights Standards, *supra* note 57. Without such a change, a sizable delay and burden on pharmacies and patients could occur. Patients would have to visit the pharmacy to sign the consent form, wait for the prescription to be filled and then return to pick up their prescriptions at

2. Authorization for Disclosure and Use Not Related to Health Care

A different consent model for disclosures and uses of PHI unrelated to health care is employed in the rule. Such disclosures of PHI may be made for employment decisions or the evaluation of credit status. Prior to using or disclosing PHI for non-health care purposes, covered entities must obtain an authorization from the individual. The authorization, unlike the written consent required for health care purposes, contains specific information to help individuals decide whether to permit disclosure or use. Such authorizations must (1) identify the information to be used or disclosed in a "specific and meaningful fashion;"[101] (2) provide the names of the persons or organizations who will make and receive the use or disclosures;[102] (3) explain the purpose for each request;[103] (4) notify the individual of his right to refuse to sign the authorization without negative consequences to treatment or health plan eligibility (except under specific circumstances);[104] (5) be written in plain language[105] and feature an expiration date;[106] and (6) explain that the individual has a right to revoke the authorization[107] at any time in writing except regarding actions taken by the covered entity in reliance of the authorization.[108] This authorization process better protects patients' privacy than the written consent requirement because covered entities generally may not condition treatment or insurance enrollment on a patient's signature of the authorization.[109]

the pharmacies, while the pharmacies would have to devise a method to store and process the consents. *See* Gostin, *Regulations under HIPAA*, *supra* note 86, at 3017.

101. § 164.508(c)(1)(i).

102. § 164.508(c)(1)(ii)-(iii).

103. § 164.508(d)(1)(ii).

104. § 164.508(e)(1).

105. § 164.508(c)(2).

106. § 164.508(c)(1)(iv).

107. § 164.508(c)(1)(v)-(vi).

108. § 164.508(b)(5)(i).

109. § 164.508(b)(4). There are some limited exceptions. One is that health care providers may condition provision of research-related treatment on authorization. §164.508(b)(4)(i). Another is that if the covered entity is gathering individually-identifiable health information solely for the purposes of disclosing it to a third party, such as an employer, the covered entity may condition this care on the authorization to disclose it to the third party. § 164.508(b)(4)(iv). Further protection is offered regarding psychotherapy notes. Authorization is always required for use and disclosure of psychotherapy notes except in specified health care operations. § 164.508(a)(2).

3. Making Exceptions: Balancing Communal Goods and Personal Privacy

The privacy rule makes several exceptions to the informed consent and authorization provisions related to the use of disclosure of PHI. These exceptions include:

a. Law Enforcement

A covered entity may disclose PHI to a law enforcement official without informed consent pursuant to a court order, subpoena or administrative request, including a civil investigative demand or an administrative subpoena.[110] Judges are given no criteria from which to make their determination as they balance individual privacy and law enforcement. In addition, a covered entity may disclose limited information[111] without prior judicial approval where: (i) the information relates to a crime victim who is incapacitated and disclosure is necessary and in the best interests of the individual;[112] (ii) PHI is evidence of "criminal conduct that occurred on the premises of the covered entity;"[113] and (iii) in the course of an emergency, disclosure is necessary to alert law enforcement to the location, commission and nature of the crime, victims or perpetrators.[114]

b. Judicial and Administrative Proceedings

PHI may be disclosed in any judicial or administrative proceeding without the person's permission in response to an order of the court overseeing the proceeding.[115] As in the law enforcement context, judges are given no criteria in the rule to exercise their discretion. Covered entities may also disclose health information in response to a subpoena or discovery request if the

110. *See* § 164.512(f)(1). When an administrative request is utilized, the rule lays out certain requirements: (1) the information sought must be "relevant and material to a legitimate law enforcement inquiry;" (2) the request must be "specific and limited in scope to the extent reasonably practicable;" and (3) de-identified information must not be able to be reasonably used. § 164.512(f)(1)(C).

111. § 164.512(f)(2)(i). The permitted information is name, address, date and place of birth, social security number, blood type, type of injury, date and time of treatment and a description of distinguishing characteristics. *Id.*

112. § 164.512(f)(3). The specific criteria are: (1) the law enforcement official represents that the information is needed to determine whether a crime occurred by an individual other than the victim and that the information will not be used against the victim; (2) the law enforcement official represents that immediate law enforcement activities would be jeopardized by waiting for consent; and (3) the covered entity determines that the disclosure is in the best interest of the individual. § 164.512(f)(3)(iii). If the patient is competent and no emergency exists, the patient must agree under the exception for the disclosure to occur. § 164.512(f)(3)(i).

113. § 164.512(f)(5).

114. § 164.512(f)(6).

115. § 164.512(e).

requester (i) reasonably attempts to inform the patient of the disclosure;[116] or (ii) reasonably attempts to obtain a protective order to prohibit the recipients from using or disclosing the information for purposes other than the litigation.[117] Instead of placing the burden on litigants seeking the information, the rule requires that patients make objections to the court.

c. Minors

Disclosures to parents of unemancipated minors are exempted from consent requirements in multiple cases. If state law forbids *or requires* that parents be informed about their children's health conditions, the rule allows state law to stand.[118] While many states permit competent minors to receive medical treatment for potentially stigmatizing conditions without parental consent,[119] states could pass laws requiring parents to be informed about their child's condition and treatment. Where no state law exists, the rule allows parents to serve as personal representatives,[120] who generally can act on behalf of the individual[121] child under some restrictions.[122] The Bush Administration has suggested that it may modify the rule to increase parental access.[123]

116. § 164.512(e)(1)(ii)(A). The covered entity must obtain satisfactory assurances that the party requesting information has made a good faith attempt to provide written notice to the individual and that the notice included sufficient information about the litigation to permit the individual to raise an objection in the proceedings. § 164.512(e)(1)(iii)(A) & (B). The covered entity must also be given assurances that the time for the individual to raise objections to the court has elapsed and that any objections given were resolved in the favor of the requester. § 164.512(e)(1)(iii)(C).

117. § 164.512(e)(1)(ii)(B). The party requesting information must give the covered entity satisfactory assurances that the parties have agreed to a qualified protective order or that the requester has asked for a qualified protected order. § 164.512(e)(1)(iv). The standard defines qualified protective order as one that prohibits the parties from using or disclosing PHI for any purpose other than litigation or proceeding for which the information was requested and requires the PHI's return to the covered entity or destruction at the end of the proceeding. § 164.512(e)(1)(v).

118. *See* § 160.202 (defining "more stringent").

119. *See* Gostin, *Regulations under HIPAA*, *supra* note 86, at 3017.

120. *See* § 164.502(g)(1).

121. § 164.502(g)(2).

122. § 164.502(g)(3). If the minor consents to the health care service, the parent agrees to confidentiality between provider and the minor, or if the minor consents and does not wish the parent to be the personal representative, then the parent is not considered a personal representative. *Id.*

123. *See* Press Release, Secretary Thompson, *supra* note 2 ("we will make it clear through guidelines or recommended modifications that . . . parents will have access to information about the health and well-being of their children, including information about mental health, substance abuse or abortion"). *Id.* The July, 2001 guidance indicated the Secretary is still considering such action. *See* Office for Civil Rights Standards, *supra* note 57 (referring to statements in the section on "Parents and Minors").

d. "Significant Others" of Adults and Emancipated Minors

Disclosures to "significant others" (meaning family, friends, caretakers or health care surrogates) of adults and emancipated minors are narrowly exempted. Covered entities may disclose limited health information to "significant others" without consent if the patient is informed in advance and has the opportunity to agree.[124] The disclosed PHI must be (i) directly relevant to the person's involvement with the patient's care or payment for care;[125] or (ii) used to notify that person of the patient's location, general health condition, or death.[126] In cases of incapacitation or emergency, disclosures to "significant others" may be made in the patient's best interest when directly relevant to the entity's involvement with the individual's care.[127]

e. Public Health

The health data privacy rule broadly exempts[128] disclosures of PHI for routine public health activities.[129] This includes disclosures: (i) where federal or state law authorizes public health authorities[130] to collect PHI to prevent or control disease, injury or disability, or report child abuse or neglect; (ii) to notify persons who may be at risk for or exposed to a communicable disease (for instance, partner notification provisions);[131] (iii) concerning adverse events, tracks and recalls of products, and post marketing surveillance by persons subject to the jurisdiction of the Food and Drug Administration.[132] State reporting or other public health laws that offer more stringent privacy protections are not preempted by the rule.[133]

f. Health Research

Most federally-funded human subject research is currently governed by a federal regulation known as the Common Rule,[134] which does not contain

124. *See* 45 C.F.R. § 164.510(b)(1) & (2) (2001). Disclosure is also permitted if the covered entity can reasonably infer from the circumstances that the patient does not object to disclosure. *See* § 164.510(b)(2)(iii).

125. § 164.510(b)(1)(i).

126. § 164.510(b)(1)(ii).

127. § 164.510(b)(3). The rule allows relatives and close personal friends to perform common care-taking duties such as picking up prescriptions, medical supplies, et cetera. *Id.*

128. § 164.514(b)(2) (clarifying that all of the exceptions apply to uses of PHI, as well as disclosures in the public health exemptions section).

129. *See* Gostin, *Regulations under HIPAA*, *supra* note 86, at 3019.

130. Public health authority is expansively defined as a federal, tribal, state or local agency or authority, or a person or entity with a grant of authority from or contract with the agency that is responsible for public health matters as part of its official mandate. 45 C.F.R. § 164.501.

131. § 164.512(b)(1)(i)(ii), (iv).

132. § 164.512(b)(1)(iii), (v).

133. § 160.203(b).

134. Protection of Human Subjects, 56 Fed. Reg. 28003 (1991) (codified at 45 C.F.R. pt. 46).

detailed privacy standards. Rather, this rule conditions institutional review board (IRB) approval of research on whether "there are adequate provisions to protect the privacy of subjects . . . ."[135] Though the Common Rule is a helpful guide for protecting the privacy and other ethical interests of human research subjects, it does not apply to privately-funded research. The health data privacy rule closes this gap between the federal and private sectors by providing more detailed requirements than the Common Rule. A covered entity may only use or disclose PHI for research without the person's permission if it obtains a waiver from an IRB or privacy board[136] that finds: (i) the use or disclosure involves no more than minimal risk; (ii) the waiver will not adversely affect the privacy rights and welfare of the individuals; (iii) the research could not practicably be conducted without the waiver; (iv) the research could not be conducted without the protected health information; (v) the privacy risks are reasonable in relation to the anticipated benefits, if any, to individuals and the importance of the research; (vi) a plan exists to protect the identifiable information from improper use and disclosure; (vii) a plan to destroy the identifiers exists unless there is a health or research justification for retaining them; and (viii) there are written assurances that the data will not be reused or disclosed to others, except for research that would also qualify for a waiver.[137] Researchers must also show that PHI is necessary for the research, will not be disclosed to outsiders and is sought solely to prepare for the research.[138] While certain critics are concerned about the burdens imposed by the new requirements,[139] the standard fairly ensures that there are valid justifications for utilizing PHI for research without consent.

g. Commercial Marketing

In contrast to some of the other exceptions, which offer either greater or similar protections than the law currently provides, the exception for

135. Protection of Human Subjects, 45 C.F.R. § 46.111(a)(7). In the Common Rule, if consent is required, the researcher must provide the subject with "[a] statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained . . . ." 45 C.F.R. § 46.116(a)(5). The Common Rule also applies to research conducted in anticipation of Food and Drug Administration approval.

136. § 164.512(i)(1)(i). The privacy board must have members with varying backgrounds, appropriate professional competency and no conflict of interest. § 164.512(i)(1)(i)(B). At least one member must be unaffiliated with the covered entity and research entity. § 164.512(i)(1)(i)(B)(2). This includes relatives of individuals affiliated with the organizations. *Id.* A majority of the privacy board must be present when considering a waiver, including the unaffiliated member. § 164.512(i)(2)(iv)(B).

137. § 164.512(i)(2)(ii).

138. § 164.512(i)(1)(ii). *See* Mark Barnes & Sara Krauss, *The Effect of HIPAA on Human Subject Research*, 10 HEALTH L. REP. 1026, 1030-31 (2001).

139. *See, e.g.*, Barnes & Krauss, *supra* note 138, at 1031 (arguing that IRB's are ill-prepared to make the assessments now required of them by the health data privacy rule).

commercial marketing provides for less privacy protection by condoning the use or disclosure of PHI for commercial marketing without consent.[140] PHI may be used or disclosed without consent for marketing communications to the individual that occur in face-to-face encounters (whether health-related or not), concern products or services of nominal value, or concern health-related products and services of the covered entity or a third party.[141] A covered entity may target persons based on their health status if the product or service may be beneficial to them.[142] Thus, under this exception, a non-physician salesperson can approach individuals with potentially stigmatizing conditions (such as HIV, pregnancy or mental illness) at their residences and inform them that he learned of their illness without their consent and would like to sell or offer information about a product.

4. Principles to Guide Disclosure Exceptions

Many of these exceptions sacrifice individual autonomy regarding personal privacy interests for the sake of communal goods and commercial interests. In certain contexts, such trade-offs may be appropriate, especially when HHS's broader goal of enhancing the health of the population is achieved. Yet, as with many existing health information privacy laws, some disclosure exceptions to an informed consent requirement lack credibility and may be ethically unsound. Exceptions in a health information privacy statute must be ethically justified to enhance individual trust in the health care system and improve health outcomes, consistent with the following principles:

a. Further Health Care Purposes

While most exchanges of health data in the electronic health information infrastructure should be made only after an individual's consent, some disclosures may be justifiable without informed consent when made for health-related purposes. Disallowing such disclosures could negate advancements in individual or populational health outcomes by denying access to health data to persons with a legitimate need to know. Public health and research activities clearly advance this aim, as do limited disclosures to "significant others" in the case of medical emergencies or basic care-taking activities (such as picking up prescriptions or X-rays). In contrast, exemptions for law enforcement, judicial and administrative proceedings and commercial marketing do not serve to improve individual and public health outcomes.

140. Robert Gellman, *Analysis of the Marketing Provisions of the HIPAA Privacy Rules*, *available at* http://www.hipaadvisory.com/action/privacy/marketing.htm (last modified Jan. 2001).

141. § 164.514(e)(2).

142. § 164.514(e)(3)(ii)(A).

b. Operate in the Individual's Best Interest

Ethical principles support non-consensual disclosures made to directly benefit the subject of PHI through the delivery of clinical care or the provision of other health services (such as the disclosure exception for "significant others" of adults or emancipated minors whose best interests are explicitly considered by the covered entity in case of emergency or the patient's incapacity). Of less benefit is the ability of parents to obtain PHI of minors regarding treatment for potentially stigmatizing conditions such as pregnancy or sexually-transmitted diseases where state laws permit such disclosures. Minors fearing punishment may avoid treatment to the detriment of their individual well-being. Avoiding treatment might also result from exceptions for law enforcement and judicial and administrative proceedings, where PHI can ultimately be used to punish individuals (such as for criminal actions) or reduce judicial remedies (for example, in workers' compensation cases to show a pre-disposition to a relevant injury).[143]

c. Promote Communal Health While Minimally Threatening Individual Privacy

Where the benefits of public health and research relate to society, as well as individuals, non-consensual disclosures of PHI for such communal, health-related goods (such as public health and health research) are justified. Public health practice has traditionally relied on these disclosures as authorized through federal, state and local laws. Human research (in some cases) may necessitate the need to use PHI without informed consent. Though the autonomous interests of the individual are infringed through these disclosures, the utilitarian premise that individuals should contribute to these greater goods in society sustains these types of disclosures.

d. Disregard Commercial Interests of Health Care Industry

Like public health authorities and researchers, private industry (health insurers, pharmaceutical companies and medical products providers, for instance) may claim a need for PHI to provide products, services or knowledge that improve individual and communal health. In some cases, these claims are legitimate. However, where access to PHI is undergirded by profit-oriented goals of recipients in the private sector (as contrasted with the community-oriented goals of government or academic researchers), the claim for non-consensual access to PHI is unjustified. People may choose to participate in private sector research or marketing campaigns, but should not have to. The commercial marketing exception unacceptably permits broad disclosures based on a pure profit motive before individuals have a chance to object.

143. *See* Hodge, *supra* note 87, at 120.

C. Privacy and Security Policies for Covered Entities

In addition to an individual's right to control uses and disclosures, the development of privacy and security policies for covered entities is important to prevent privacy breaches and maintain consumers' trust in the health care system. Without such policies, accidental disclosures from sloppy record keeping and purposeful disclosures by and to unscrupulous parties may proliferate.[144] Addressing these concerns, the health data privacy rule mandates that covered entities develop privacy and security policies while maintaining the flexibility necessary for the large variety of participants covered by the rule.[145] Covered entities must implement policies that reasonably protect from any "intentional or unintentional use or disclosure in violation of the standards, implementation specifications or other requirements."[146] Covered entities must not only guard against a deliberate attempt to use protected information, but also must endeavor to prevent accidental uses and disclosures. Procedures must be developed to allow for complaints about the policies or the covered entities' compliance with the policies.[147] Staff members who violate privacy policies may be sanctioned.[148]

A covered entity may not require an individual to waive these rights in order to receive care, enroll in a health plan or obtain benefits.[149] However, covered entities are not mandated to create a formal appeals process or a form of "due process."[150] When violations occur, the covered entity must mitigate "to the extent practicable" any harmful effect known to result from the infraction.[151]

144. For more on the impact on personal privacy from security policies, see HEALTH PRIVACY PROJECT, BEST PRINCIPLES, *supra* note 72, at 20-22.

145. Specific concerns calling for flexibility include that the nature of the health information held by covered entities may differ, smaller organizations may be burdened greatly by requirements more appropriate for larger firms and the swift changes in technology may require a fast process to update the privacy and security policies. *See* Gostin, *Health Information Privacy*, *supra* note 4, at 526.

146. 45 C.F.R. § 164.530(c)(2) (2001). Group health plans that provide benefits only through a health maintenance organization (HMO) or an issuer and that do not create, receive or maintain PHI are not subject to any of the requirements under this section except documentation of their plan materials. § 164.530(k). The issuers and HMOs must still follow all of the elements of the privacy and security policy mandates. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,563-64 (Dec. 28, 2000).

147. § 164.530(d). Covered entities are also forbidden from taking any "intimidating or retaliatory acts" against an individual involved in the privacy policy process, including those filing a complaint. § 164.530(g).

148. § 164.530(e)(1).

149. § 164.530(h).

150. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,562 (Dec. 28, 2000).

151. § 164.530(f). Balancing the protections for individuals requires flexibility for businesses. Every covered entity is not compelled to develop the same privacy and security

D. Fair Information Practices

Persons and entities maintaining PHI must adhere to a range of fair information practices that allow individuals to make informed choices about the delivery and financing of their health care. The health data privacy rule proscribes several fair information practices for health consumers.

1. Notice

Health care consumers have the right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity.[152] Individuals are also entitled to know their rights and the covered entity's legal duties regarding the new privacy and security policies and fair information practices requirements.[153] The notice must be in plain language to prevent covered entities from employing legal language that may confuse individuals.[154] The type of notice required is determined by the nature of the covered entity.[155] Several consumer safeguards apply to covered entities that pursue electronic notice.[156]

---

policies. Instead, the policies must be "reasonably designed, taking into account the size of and the type of activities that relate to PHI undertaken by the covered entity." § 164.530(i)(1). This generalized description of the requirement allows small businesses to develop plans that reflect the nature and size of their enterprise without burdening them more than necessary. Small businesses might still find some of the requirements overly burdensome. For example, a sole practitioner largely relying on paper medical records might be challenged by the need to prevent accidental disclosure from a misplaced record. As the health data privacy rule mandates that covered entities' privacy policies "promptly" comply with changes in law, further difficulties can arise to small businesses with limited resources to monitor legal developments and implement swift changes. § 164.530(i)(3). *See also* Gostin, *Regulations under HIPAA*, *supra* note 86, at 3018.

152. § 164.520(a)(1). For more on the necessity of providing such notice, see Gostin, *Health Information Privacy*, *supra* note 4, at 522-24; HEALTH PRIVACY PROJECT, BEST PRINCIPLES, *supra* note 72, at 19-20.

153. § 164.520(a)(1). The notice must include information about how individuals may complain about potential misuses or violations to the covered entity and the Secretary of HHS or contact the covered entity with questions. § 164.520(b)(1)(vi).

154. § 164.520(b)(1).

155. § 162.520(c)(1), (2). Health plans must provide notice to covered individuals by the compliance date of the regulation. New enrollees must get the notice at the time of enrollment. At least once every three years, the health plan must notify enrollees in the plan that the notice is available and the methods by which they can obtain it. § 164.520(c)(1). In contrast, health care providers have to provide the notice upon the first service delivery after the compliance date. § 164.520(c)(2).

156. An individual must agree to obtain the notice via e-mail. A paper copy must be provided if the covered entity knows that the e-mail transmission failed. § 164.520(c)(3)(ii). Health care providers must give electronic notice automatically and simultaneously when their first service delivery is electronic. § 164.520(c)(3)(iii). If a covered entity maintains a web site that offers information about its benefits and services, it must also prominently post its notice on the web site as well as make it available electronically. § 164.520(c)(3)(i).

2. Access to Protected Health Information

The new regulation offers individuals a broad opportunity to access their PHI.[157] Access rights include an on-site inspection of the records and the provision of copies.[158] Covered entities must act within thirty days upon the request.[159] If the individual agrees in advance, the covered entity may provide a summary of the PHI instead of the actual documents.[160] The standard does permit narrow reasons that cannot be reviewed for denial regarding requests for psychotherapy notes; information likely to be used in a civil, criminal or administrative proceeding; and requests by inmates to their correctional facility or health care provider that might threaten the health or safety of the individual or others.[161] Also, in limited circumstances,[162] a covered entity may deny access as long as the individual may request a review of the grounds for denial.[163] If the covered entity decides to deny access to the individual of any part of the PHI, the rule ensures a fair and informed process.[164]

157. § 164.524 (2001). The covered entity may require the request be in writing. § 164.524(b)(1). For more on the significance of the individual's ability to access their personal medical data, see Gostin, *Health Information Privacy*, *supra* note 4, at 524; HEALTH PRIVACY PROJECT, BEST PRINCIPLES, *supra* note 72, at 18-19.

158. § 164.524(c)(1).

159. *Id.* § 164.524(b)(2)(i). Sixty days is allowed if the information is held off-site. § 164.524(b)(2)(ii). Delay is also allowed if the covered entity informs the individual in writing of the reasons it requires more time and when the request will be granted. § 164.524(b)(2)(iii).

160. § 164.524(c)(2)(ii).

161. § 164.524(a)(1), (2). Information obtained from another based on a promise of confidentiality and that would likely reveal the identity of the source may be denied without review. § 164.524(a)(2)(v). Also, health care providers may temporarily deny access during research based on an individual's care if the individual has consented to the research, and the denial of access occurs during research. § 164.524(a)(2)(iii).

162. These situations include where a licensed health care professional determines that access will endanger the life or physical safety of the individual or another person. § 164.524(c)(3).

163. *Id.* This provision specifically covers determinations that references to another person will endanger that other individual, or that, if a personal representative is making the request, substantial harm will come to the individual or another person. § 164.524(c)(3).

164. The denial must be in writing and in plain language. It must explain the reasons for the denial, any rights for review over the decision and methods of complaint to the covered entity. § 164.524(d)(2). Access should be granted to any information that does not meet the specific grounds for denial. § 164.524(d)(1). If a review of the denial is warranted, it is conducted by a licensed health care professional who is designated by the covered entity but is not directly involved in the decision to deny access. § 164.524(d)(4).

3. Amend Protected Health Information

Individuals may amend their PHI if they note inaccuracies or missing information.[165] The covered entity must act within sixty days on a request to amend.[166] If the covered entity agrees to the amendment, it must (a) identify the records that are affected by the amendment, (b) append or provide a link to the amendment[167] and (c) inform the individual of the amendment.[168] Additional covered entities who possess or receive the data must amend their records with the corrected information about the relevant individual.[169] As with access rights, covered entities may deny amendments in certain circumstances, including upon a determination that the record is "accurate and complete."[170] The entity must give written notice to the individual upon denial of a request for an amendment.[171] Should the individual disagree in writing,[172] the covered entity can respond with a written rebuttal.[173] Yet, unlike disputes over denial to access, there is no final review to clarify which party, the individual or the covered entity, is correct.

165. § 164.526(a)(1). See Gostin, *Health Information Privacy*, *supra* note 4, at 524 and HEALTH PRIVACY PROJECT, BEST PRINCIPLES, *supra* note 72, at 18-19, for more on the significance of this right.

166. § 164.526(b)(2)(i). An extension of thirty days is possible if the covered entity explains the reasons for delay and the date on which it will respond to the request in writing to the individual. § 164.526(b)(2)(ii).

167. § 164.526(c)(1), (2).

168. § 164.526(c)(2), (3). It must also notify persons or entities (1) identified by the individual as needing the amended information; or (2) known by the covered entity to have PHI about the individual and who may rely on the information to the detriment of the individual. *Id.*

169. § 164.526(e).

170. § 164.526(a)(2)(iv). Other grounds for denial are: (1) if the covered entity did not create the information or record, it may deny the request unless the individual reasonably shows that the originator of the information is no longer available to address the amendment request and (2) if the individual could not access the record because of restrictions laid out in § 164.524 (*see* Part II.D.1 above), the covered entity would have grounds to deny the amendment. § 164.526(a)(2)(i), (iii).

171. § 164.526(d)(1). It must be in plain language and explain the reasons for the denial, any rights for review over the decision and methods of complaint to the covered entity. § 164.526(d)(1)(i)-(iv).

172. § 164.526(d)(2).

173. § 164.526(d)(3). The individual must be provided with a copy of the rebuttal. The written statement and rebuttal must then be appended or linked to the appropriate records by the covered entity (§ 164.526(d)(4)) and included, when relevant, in any future disclosures. § 164.526(d)(5)(i). If the individual has not submitted a written statement of disagreement, then the request for amendment and covered entity's denial must be included if the individual has requested such disclosure. § 164.526(d)(5)(ii).

4. Request an Accounting of Disclosures

Patients have a limited right to receive an accounting of disclosures of their PHI (other than for disclosures related to treatment, payment and health care operations, among other exceptions[174]) over the six year period prior to the request.[175] The accounting includes the name of the person or entity who received the information (and their address if known), the date of the disclosure, a brief description of the information disclosed and a brief explanation of the reasons for disclosure if not authorized by the patient.[176]

E. The Effects of Pre-emption

Under HIPAA, HHS cannot preempt state health information privacy laws that are more protective of patients than the national rule.[177] For this reason, the rule sets a federal "floor" of protections. Some states may offer more protections through, for example, "super-confidentiality" laws for genetic, mental health or HIV/AIDS information.[178] This multi-level approach to protecting privacy has at least two disadvantages: (1) it unfairly allows individuals in some states to benefit from greater privacy protections than in other states; and (2) where most electronic health data is exchanged across state boundaries, covered entities (specifically larger health providers, plans and clearinghouses) must adhere to both national and regional privacy standards. This likely results in higher costs than would occur if a uniform national standard was in place.[179]

III. CONCLUSION

The systematic electronic collection, use and disclosure of individually-identifiable health information are essential to achieving several important communal goals. Public health authorities and health researchers require such data to perform accurate, beneficial studies and to shape effective interventions and treatments. The exchange of electronic data can improve clinical outcomes, prevent fraud and abuse, and help consumers make informed choices about their health care. With these positive aspects, however, come significant threats to individual privacy. People are concerned about

174. These include: national security and intelligence purposes; correctional institutions; and health oversight agencies or law enforcement officials who document that the agency's officials would be impeded if the accounting revealed the disclosure. § 164.528(a)(1), (2).

175. § 164.528(a)(1).

176. § 164.528(b)(2)(i)-(iv).

177. § 160.203(b). State laws are also not pre-empted if they promote certain goods such as public health, efficacy in payment of health care, fraud prevention and audits and program monitoring. § 160.203(a)(1)(i), (iv), (d).

178. *See* Gostin, *Regulations under HIPAA*, *supra* note 86, at 3020.

179. *See id.*

discrimination and autonomy violations that follow unwarranted disclosures to health insurers, employers and governmental agencies.

Through its health information privacy rule, HHS seeks to provide a national standard that balances individual interests in health information privacy with society's interests in accomplishing various communal goals. The rule provides expansive, new protections for health data privacy and security. In many ways it improves existing privacy protections by creating a more fair and even field in which information can be responsibly exchanged. Unfortunately, the rule fails to provide a sufficient floor of protection for the use and disclosure of all health information. Limited by Congressional authorization under HIPAA, HHS at times trades personal privacy for public (such as the public health exception) and non-public goods (such as the commercial marketing exception). Reaching a proper balance between individual and communal uses of health data may require additional authorization from Congress, or alternatively, new federal legislation. For now, the rule represents a new standard in an age of increasing threats to individual interests in protecting the privacy of their health data.